AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously presented) A computer implemented method for managing security risk, the method comprising:

setting in a computer storage a hierarchical relationship between two or more elements comprising an entity wherein a first element comprises a physical facility and a second element subordinate to the first element comprises a resource located at the physical facility;

receiving into the computer storage on a real time basis an indication of a security risk associated with one or more of the first or second elements, wherein the indication of a security risk comprises at least one of: a potential for physical, reputational, economic or legal harm to the resource and is received from government agency or a news feed;

receiving digital data into the computer storage from the government agency or news feed; wherein the digital data is descriptive of the security risk;

receiving into the computer storage an indication of a selection of the first or second element; and

transmitting via a computer processor coupled to a communication network apparatus, the data descriptive of the security risk as it relates to the element selected and the other element, based upon the hierarchical relationship of the elements and the indication of the security risk.

2. (Previously presented) The method of claim 1 additionally comprising the steps of generating a list of resources with the element selected and transmitting the list of resources.

3. (Previously presented) The method of claim 1 wherein the first or second element selected comprises a geographic area delineated according to at least one of: a national boundary, and a political boundary.

4. (Original) The method of claim 1 wherein the description of the security risk as it relates to the element selected comprises at least one of: a threat of physical harm to an asset; a threat of misappropriation of an asset; and a threat of physical harm to one or more persons.

5. (Previously presented) The method of claim 1 wherein the description of the security risk as it relates to the element selected comprises misappropriation of information comprising data stored in a computerized information system.

6. (Previously presented) The method of claim 1 additionally comprising the step of transmitting via a computer processor coupled to a communication network, a subjective quantifier descriptive of an amount of harm that could be caused by the security risk.

7. (Previously presented) The method of claim 1 additionally comprising the step of transmitting via a computer process coupled to a communication network, a subjective quantifier descriptive of a time frame during which harm, caused nut he security risk, could be experienced by an associated element.

8. (Original) The method of claim 1 wherein the hierarchical relationship between two or more elements comprises a progressively greater or lesser resolution ranging from a country level resolution to a room level resolution.

9. (Previously presented) The method of claim 1 additionally comprising the step of receiving into the computer storage an image of an element and transmitting via a computer processor coupled to a communication network the image with the description of the security risk as it relates to the element selected.

10. (Previously presented) The method of claim 1 additionally comprising the steps of: color coding elements and associated risks with a computer processor and storing and indication of the coded elements and associated risks in the computer storage, according to at least one of: a degree of risk, a type of risk, a type of element; a value of assets involved and propensity for the risk to grow.

11-14. (Cancelled)

15. (Previously presented) A computerized system for or managing security risk, the system comprising:

a computer server accessible with a system access device via a communications network; and

executable software stored on the server and executable on demand, the software operative with the server to cause the server to:

set a hierarchical relationship in a computer storage between two or more elements comprising an entity wherein a first element comprises a physical facility and a second element subordinate to the first element comprises a resource located at the physical facility;

receive into the computer storage an indication of a security risk associated with one or more of the first or second elements wherein the indication of a security risk comprises at least one of: a potential for physical, reputational, economic or legal harm to the resource and is received from government agency or a news feed;

receive digital data into the computer memory from the government agency or news feed, wherein the digital data is descriptive of the security risk;

receive into the computer storage an indication of a selection of the first or second element; and

transmit via a computer processor coupled to a communication network, the data descriptive of the security risk as it relates to the element selected, based upon the hierarchical relationship of elements and the indication of the security risk.

16. (Previously presented) Computer executable program code residing on a computer-readable medium, the program code comprising instructions for causing the computer to:

set a hierarchical relationship in a computer storage between two or more elements comprising an entity wherein a first element comprises a physical facility and a second element subordinate to the first element comprises a resource located at the physical facility;

receive into the computer storage on a real time basis an indication of a security risk associated with one or more of the first or second elements wherein the indication of a security risk comprises at least one of: a potential for physical, reputational, economic or legal harm to the resource and is received from government agency or a news feed;

receive digital data into the computer memory from the government agency or news feed, wherein the digital data is descriptive of the security risk;

receive into the computer storage an indication of a section of the first or second element; and

transmit via a computer processor coupled to a communication network, the data descriptive of the security risk as it relates to the element selected, based upon the hierarchical relationship of elements and the indication of the security risk.

17. (Cancelled)

18. (Cancelled)